REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars:

Claim for foreign priority

The examiner has not acknowledged Applicant's claim for foreign priority or receipt of the priority documents. The examiner is requested to review the Declaration filed with the present application which indicates that foreign priority benefit of German application 19935945.8 is claimed. Further, Applicant notes that the priority document is part of the application record and can be found in the Image File Wrapper identified as "Foreign Priority Papers filed" and dated January 30, 2002.

Applicant respectfully requests acknowledgement of the priority request and receipt of the priority document in the next communication.

Objections to the specification

The specification is objected to because the application does not contain an abstract, and because appropriate section headings are omitted.

An abstract is provided herewith, and the specification has been amended to include appropriate section headings. In view of these amendments, withdrawal of the objection is respectfully requested.

Rejection of claims 1, 4, and 7 under 35 U.S.C. § 112, second paragraph

Claims 1, 4, and 7 presently stand rejected as being indefinite. The examiner notes that the claims recite the term "and/or." Also, the examiner identifies the use of the phrase "with respect to" in claim 4 as unclear, and suggests that it appears that at least two authentication processes are being recited.

Claims 1, 4, and 7 have been amended to remove the term "and/or." Claim 4 has been amended to eliminate the recitation of "with respect to," and to more clearly set forth two aspects of the authentication process (one of authenticating that a terminal is

authorized for use with the data carrier, and one of authenticating that the user is authorized to use the data carrier). The claims have been further amended in the interest of clarity and conformance with U.S. practices.

Rejection of claims 1-9 under 35 U.S.C. § 103(a)

Claims 1-9 presently stand rejected as being unpatentable over Boerbert (U.S. 5,272,754). This rejection is respectfully traversed for the following reasons.

Claim 1 has been amended to more clearly recite a method for authenticating a user of a data carrier for authorized use of the data carrier and for authenticating a data carrier terminal for authorized access by the data carrier terminal of memory areas of the data carrier.

The method comprises the steps of reading a secret code from the data carrier by the data carrier terminal, wherein the secret code is only accessible by authorized data terminals (based on specific location or encryption of the secret code known only to authorized terminals). The read secret code is then presented to the user (on the data carrier terminal) for the user's evaluation for correctness. Only after receiving an indication that the presented read secret code is correct, the data carrier terminal reads a biometric feature presented by the user, and the presented biometric feature is compared with a biometric feature stored in the data carrier to authenticate that the user is authorized to use the data carrier.

It is respectfully submitted that Boerbert fails to disclose or suggest each and every element set forth in claim 1 of the present application. Boerbert fails to disclose or suggest a method wherein a data carrier terminal reads a secret code from a data carrier, and then ***presents*** (displays) ***the secret code*** for verification by the user, and then, only upon an ***indication by the user*** that the secret code is correct reads biometric data of a biometric feature presented by the user.

Instead, Boerbert discloses a method related to security in communication between a computer and a terminal. Such security is obtained by means of a user token. The user presents the token to a reading device and is asked to present a PIN. Next, a controller

builds a message containing the PIN, the name of the user, an access authorization, and a "last countersign." This message is sent to the computer, which verifies the message. If the PIN or "last countersign" are not as expected, the user is not authorized for use of the computer. However, there is no teaching or suggestion that the PIN (or the "last countersign" or a secret code or any other data item) is ***presented to the user*** for verification prior to a ***subsequent step*** for authenticating the user based on a biometric feature (or any further feature).

While the examiner asserts that Boerbert discloses "presenting the read secret code to the user, where the code presented is the token information which is the countersign," it must be noted that the only teaching regarding displaying the countersign, based on the flowchart of Fig. 6 and the discussion at Col. 11, lines 3-11 cited by the examiner, suggests that the countersign is only displayed ***after*** the completion of the authentication process. There is no teaching or suggestion that the countersign is presented for evaluation by the user, and that after receiving an indication by the user that the presented countersign is correct a further authentication step is performed wherein the terminal reads a biometric feature presented by the user for user authentication.

It must be noted that the countersign is generated by the computer, and is changed each time a user accesses the computer. This allows identification during the next access of whether the token has illegally been used in the mean time. In such a case, the countersign read from the user token no longer matches an expected "last countersign." This is clearly in contrast with the secret code of the present invention which is provided by, and is known only to, the user. Thus, while Boerbert displays the countersign (***after*** completion of the authentication process), the user is not allowed to authenticate the terminal by verifying the correctness of a displayed secret code.

It is respectfully submitted that, for at least these reasons, claim 1, and claims 2 and 3 which depend from claim 1, are allowable over the cited reference.

Claims 4 and 7 correspond to a data carrier and an authentication system, respectively, according to the method described in the application and set forth in claim 1

of the present application. It is respectfully submitted that claims 4 and 7 are allowable for the same reasons as discussed with respect to claim 1.

Further, it is noted that claim 4 has been amended to recite that the secret code can ***only be read*** by an authorized data carrier terminal (such as by specific location or encryption only known to an authorized data carrier terminal). It is respectfully submitted that Boerbert fails to disclose or suggest that a secret code is stored on the user identity token in a manner such that the secret code can be read ***only*** by an authorized data carrier terminal.

Also, claims 4 and 7 recite a data carrier having a first memory area for storing a secret code ***and*** a second memory area for storing biometric data, and claim 7 requires that the data carrier terminal has a first device for reading the secret code from the data carrier and for presenting the read secret code on a display, and a second device for reading biometric data of a biometric feature presented by a user.

While Boerbert discloses that "user authentication device 72 could include a biometric device for determining a unique physical attribute of user 23 such as fingerprints, palmprints or retinal pattern" (col. 7, lines 41-44), there is no teaching or suggestion that any biometric data is stored on the user identity token. On the contrary, it is stated that "[the biometric data] would then be sent to computer 60 during the user verification process described in FIG. 4" (col. 7, lines 44-46). Thus, it appears that a user's biometric data may be stored on the computer, not in the user identity token.

Further, there is no specific teaching or suggestion that the biometric data is used ***in addition to***, rather than ***instead of***, the PIN number stored on the user identity token. Therefore, there is no teaching or suggestion of 1) biometric data stored in a data carrier; or 2) a data carrier having a first memory area for storing a secret code ***and*** a second memory area for storing biometric data; or 3) a data carrier terminal that has both a device for reading the secret code ***and*** a device for reading biometric data.

Therefore, Boerbert fails to disclose or suggest each and every element set forth in claims 4 and 7. Accordingly, it is respectfully submitted that claims 1, 4, and 7, and their

respective dependent claims 2-3, 5-6, and 8-9, are allowable over the cited reference. Accordingly, withdrawal of the rejection is respectfully requested.

Conclusion

In view of the amendments to the claims, and in further view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-9 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date: March 14, 2006

JUSTIN J. CASSELL
Attorney for Applicants
Registration No. 46,205